

IN THE CLAIMS

Please amend the claims to read as follows:

Listing of Claims

1. (Currently Amended) A post issuance system for performing data or configuration changes within a personal security device (PSD), said system comprising:
 - said PSD, including at least one functional application and a PSD cryptographic component means,
 - a local client functionally connected to said PSD,
 - a first server functionally connected to said local client, said PSD and said first server comprising a first component means for mutual authentication, [.]
 - at least one hardware security module (HSM) HSM, including an HSM cryptographic component means complementary to said PSD cryptographic component means, said at least one HSM being functionally connected to said first server,
 - a communications pipe, established between said PSD and said at least one HSM, and
 - a storing storage component that stores or generates means for storing or generating said data or configuration changes, said storing storage component means being functionally connected to said first server, wherein:

said at least one HSM comprising comprises a controlling component that controls means for controlling said data or configuration changes sent through said communications pipe to said PSD.

2. (Currently Amended) The system according to claim 1 comprising a network for the establishment of said communications pipe.

3. (Currently Amended) The system according to claim 1 wherein said at least one functional application includes a component that processes means for processing APDU commands and said data or configuration changes received through said communications pipe.

4. (Currently Amended) The system according to claim 1 further comprising: including at least one second server in processing communications with said first server, wherein: said at least one second server includes stored data or configuration changes retrievable using a PSD unique identifier.

5. (Currently Amended) The system according to claim 4 wherein said first server and said at least one second server comprise a component means for mutual authentication.

6. (Currently Amended) The system according to claim 1 wherein said at least one functional application includes an application identifier.

7. (Currently Amended) The system according to claim 6 comprising a selecting component that selects means for selecting said at least one functional application using said application identifier.

8. (Currently Amended) The system according to claim 4 further comprising:

a network for the establishment of said communications pipe and for functionally connecting said at least one second server to said first server, and

a sending component that sends means for sending said retrieved data or configuration changes from said at least one second server over said network to said first server.

9. (Currently Amended) The system according to claim 4 wherein:

said first server comprises a first processing component
that receives and processes means for receiving and processing
said data or configuration changes, and wherein
said at least one HSM comprises a second processing
component that further processes means for further processing
said data or configuration changes.

10. (Currently Amended) The system according to claim 1 wherein said at least one HSM comprises a generating component
that generates means for generating at least one command
executable by said at least one functional application.

11. (Currently Amended) The system according to claim 10 wherein said at least one HSM comprises an encrypting component
that encrypts means for encrypting said at least one command and
said data or configuration changes, forming at least one
cryptogram.

12. (Currently Amended) The system according to claim 11
further comprising a sending component that sends means for
sending said at least one cryptogram through said communications

pipe into said PSD for processing by said at least one functional application.

13. (Currently Amended) The system according to claim 12 wherein said at least one functional application comprises:

a decrypting component that decrypts means for decrypting said cryptogram using said PSD cryptographic component means, and
an executing component that executes means for executing said at least one command.

14. (Currently Amended) The system according to claim 2 wherein said network is a public network.

15. (Currently Amended) The system according to claim 2 wherein said network is a private network.

16. (Original) The system according to claim 1 wherein said communications pipe is provided with a secure communications protocol.

17. (Currently Amended) The system according to claim 1 wherein said HSM cryptographic component means and said PSD

cryptographic component means comprise complementary asymmetric keys.

18. (Currently Amended) The system according to claim 1 wherein said HSM cryptographic component means and said PSD cryptographic component means comprise complementary symmetric keys.

19. (Currently Amended) A post issuance method for performing data or configuration changes within a personal security device (PSD), said method comprising:
establishing a communications pipe between said PSD and at least one hardware security module (HSM) HSM, wherein said PSD is functionally connected to a local client and said at least one HSM is functionally connected to a first server,
mutually authenticating said PSD and said first server,
selecting at least one functional application within said PSD associated with said existing data or configurations, [.]
generating or retrieving an HSM cryptographic component means complementary to a cryptographic component means included inside said PSD,
retrieving said data or configuration changes, [.]

processing said data or configuration changes by said first server,

encrypting said processed data or configuration changes by said at least one HSM using said complementary HSM cryptographic component means,

routing said encrypted processed data or configuration changes through said communications pipe into said PSD, and decrypting and processing said processed data or configuration changes by said at least one functional application using said PSD cryptographic component means.

20. (Currently Amended) The method according to claim 19, further comprising:

~~the step of retrieving said data or configuration changes from at least one second server, and of sending said data and configuration changes over a network from said second server to said first server.~~

21. (Currently Amended) The method according to claim 20
19 further comprising including ~~the step of mutually authenticating said at least one second server and said first server.~~

22. (Currently Amended) The method according to claim 21,
~~further comprising the further step of using a unique identifier~~
associated with said PSD for mutually authenticating said PSD and
said first server.

23. (Currently Amended) The method according to claim 19,
~~further comprising the further step of using a unique identifier~~
associated with said PSD for selecting said at least one
functional application.

24. (Currently Amended) The method according to claim 19,
~~further comprising the further step of using a unique identifier~~
associated with said PSD for generating or retrieving said HSM
cryptographic component means.

25. (Currently Amended) The method according to claim 19,
~~further comprising the further step of using a unique identifier~~
associated with said PSD for retrieving said data or
configuration changes.

26. (Currently Amended) The method according to claim 19,
wherein at least one command executable by said at least one
functional application is issued by said at least one HSM, routed

through said communications pipe into said PSD, and processed by said at least one functional application.

27. (Currently Amended) The method according to claim 19
further comprising the step of functionally connecting said local client and said first server through a private network.

28. (Currently Amended) The method according to claim 19
further comprising the step of functionally connecting said local client and said first server through a public network.

29. (Currently Amended) The method according to claim 19
further comprising the step of employing an asymmetric cryptographic component means for said HSM cryptographic component means and said PSD cryptographic means component.

30. (Currently Amended) The method according to claim 19
further comprising the step of employing a symmetric cryptographic component means for said HSM cryptographic component means and said PSD cryptographic component means.

31. (Currently Amended) The method according to claim 19
further comprising the step of using a secure communications
protocol for said communications pipe.